Plasma 白皮书

摘要

Plasma 是一个激励，和强制智能合约执行的框架。可以扩容达到每秒大量的状态更新（能达到每秒 10 亿级），在区块链上能支持全球范围内的大量的去中心化金融应用。这些智能合约通过网络交易手续费用于激励持续的自动化运作，最终依赖于底层的区块链（比如，以太坊）来强制交易状态的锁定。

我们提议的这种去中化的可扩展的自动运行应用，不仅可以用来处理金融行为，也可以通过构建面向全球的持久化数据服务的经济激励，来成为当前中心化云服务的一种备选方案。

Plasma 由两个核心部分构成：重组所有区块链计算为一组 MapReduce 函数，和一个可选的方法，在现存的区块链上，以不鼓励区块扣留的 Nakamoto 共识原则，来实现一个 Pos 的代币押金机制。

这种构建通过在主链上编写智能合约，使用欺诈证明，可以在主链上强制状态的锁定。我们将区块链编组为一个树形的分层结构，将每一个区块链视为一个独立的分支，强制将整个区块链的历史，和可 MapReduce 的计算提交到 Merkle 证明。通过主链强制将某个链的帐本信息打包到子区块链中，这个链将通过最低的信任达到不可思议的扩容（假定根链的可用性和扩展性）。

围绕全局强制非全局数据的数据可用性，区块扣留攻击是是一个非常复杂的问题。Plasms 通过对有问题链的退出机制来缓解了这个问题，同时也创建了一个激励和持续的强制的执行数据的正确性机制。

仅仅通过周期性的将正常状态的 Merkle 证明广播到主链（比如，以太坊），这将允许不可思议的扩展性，降低交易成本和计算量。Plasma 支持了大规模去中心化应用的持续运行。

1 可扩展的多方计算

在区块链中，对于正确性的校验，一般是让每个参与方自行验证每个链的正确性。为了接受一个新区块，需要参与方完整的检验区块从而保证其正确性。扩展区块交易容量的努力来自（比如，闪电网络）引入时间承诺来建立一个押金机制，（一个断言、挑战协议）这样断言的数据必须经历一个争议期后，才会真正放到区块链上来锁定状态。断言/挑战的构建过程，是允许某方断言某个特定的状态是正确的，如果断言不正确，且存在着一个争议期，争议期内，另一方可以在约定的特定时间内，提供一个证明来挑战这个断言。当出现错误的行为时，区块链可以惩罚不正当行为方。这创建了一种机制来鼓励参与方来强制执行那些不正确的断言。通过这种断言、挑战证明机制，感兴趣的参与方可以向主链上不感兴趣的各方证明某种事实（如以太坊[2][3]）。

这种结构可以不仅用于支付，也可以扩展到计算层，这样区块链作为智能拿给的裁决层。然而这种假设需要所有的参与方均是计算验证的参与方（译者注：即主链是否需要关心子链，但子链可能不使用主链货币，不需要主链的计算证明）。以闪电网络为例，这种结构可以让人们提交一个需要计算的合约状态承诺（如，通过一个树级的状态变化的预签名）。

这种结构允许可扩展的高强力计算，但也有一些问题，需要汇总一些外部的状态（比如，整个系统、市场，大量的分片、不完成状态的计算，大量贡献者的状态的汇总）。这种形式的多方离线链状态（”状态通道“）承诺，需要参与各方来提供完整的计算证有，否则有重要的信任建立在计算本身上，即使是一个单回合的模式。此外，这里引入了一个回合的假设，在合约启动前，执行的步骤是完全展开的，这给了参与方一个机会来提前退出并强制在链上进行昂贵的计算（因为不能知道哪一方有问题）。

取而代之，我们试图设计一个系统，计算可以链下发生，但最终可在链上强制执行小量的更新，使能扩展到每秒数 10 亿的计算量。这样的状态更新通过一系列自动的 Pos 验证者，他们被激励，通过欺诈证明，来促进子链上的正确的行为；从而避免单方的轻易的暂停计算服务。这将有利于减少数据可用性方面的问题（如，区块扣留问题），减少主链上的状态更新的必要，在出现 byzantine 阻止主链上的交易费的折扣风险，一种强制状态变化的机制。

与闪电网络类似，Plasma 是一系列的运行于现存区块链之上的智能合约，来强制保证大家可以可以在一个合约状态中持有资金，且能在后面的某个时间在网络上进行清算、取款。

2 Plasma

Plasma 是一种实现区块链扩容计算的方式，通过创建经济激励来实现自动和链上状态的持久化，而不需要合约创建者的裡的状态转换管理。节点自身被激励来运行一个链。

额外的，重要的可扩展性是通过减少单次花费的资金表达方式为一个位图中的一个位来实现，这样，一个交易和一个签名代表一个与多方的交易聚合。我们将这与一个 MapReduce 框架结合，同时使用含押金的智能合约来构建可扩展的计算强制性。

这种构建方式允许大家让外部的参与方持有资金，并根据自己的行为计算合约，类似于一个矿工，但是 Plasma 是运行于一个已存在的区块链上，由此大家不用在每次状态更新时在主链上创建对应的交易（即使包括添加新用户的账本），而只需要将合并后的状态变化这样的少量信息写到链上。

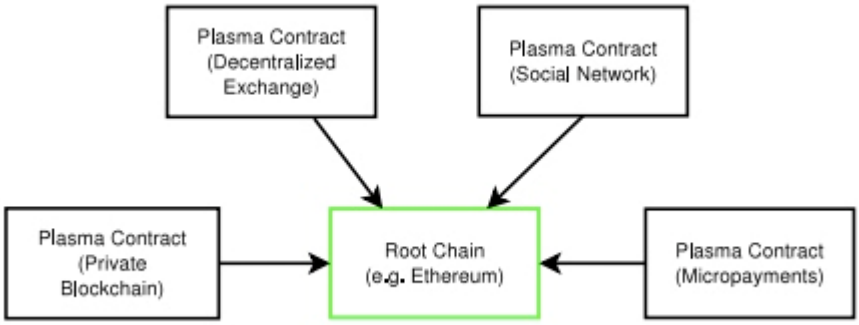
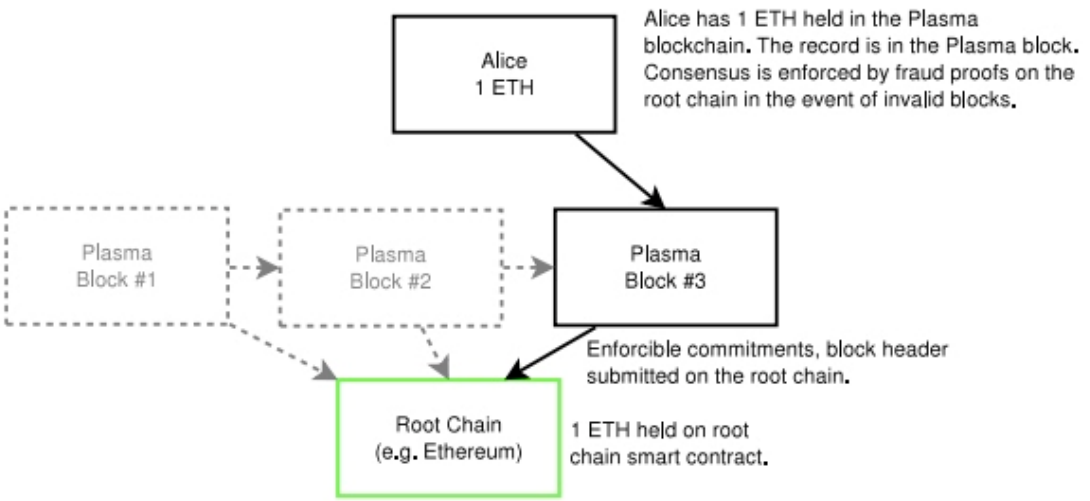


图 1：每个人都可以创建一个自定义的 Plasma 链，在不同场景下实现可扩展性。Plasma 是一系列的智能合约，允许在主链里有许多的区块链。主链可以强制 Plasma 链中的状态。主链是全局计算的强制检查者，但也只计算和惩罚那些存在欺诈的行为。许多的 Plasma 的区块链可以并存，且有他们独自的商业逻辑和合约术语。在以太坊中，Plasma 将会由 EVM 智能合约组成，并直接在以太坊上运行，但只会执行很小的几次，但可以在非 Byzantine 的情况下代表不可思议的大量计算和金融账本实体。

Plasma 由五个核心部分构成：1）一个激励层，用于持续的以优化的价格执行合约，以一种树状态形式来组织子链来尽可的提高成本效率和网络交易清算的效率，2）一个 MapReduce 框架，构建一个状态转换的的欺诈证明，在嵌套的子链中，兼容树结构同时重组状态转换为可扩展的，3）一个共识机制，依赖于主链，尝试复制 Nakamoto 共识激励，4）一个位图的 UTXO 提交结构，保证在主链下的确定的状态转换，同时尽可能降低退出费用。5）允许在数据不可用或者其它 Byzantine 行为时可以退出，也是 Plasma 的运行中的关键设计点。

2.1 Plasma 区块链，或者外化的多方通道

我们提出了一种方法，多方链下通道可以代表他人持有某个状态。我们称这个框架为一个 Plasma 区块链。对于在 Plasma 链中持有的资金，这将允许向 Plasma 链中存取资金，通过在欺诈证明中提供状态转换证明。这允许强制的状态和可互换性的存储与取款，考虑在 Plasma 块中的情况，匹配其在主链中持有的资金（Plasma 并不是设计为银行那种准备金）。



图二、Plasma 区块链是一个在区块链中的链，这个系统由押金的欺诈证明驱动强制执行。Plasma 区块链没有向主链（比如，公开链）公开自身链的内容。取而代之的是，区块的头哈希将会提交到主链，当出现需要欺诈证明的时候，然后块将回滚，区块的创建者将会受到惩罚。这将非常有效，因为许多的状态更新表示为一个哈希（加上少量的关联数据）。这个更新可以表示一个在主链上尚未显示的余额变化（Alice 在主链上没有她的账本余额，她的账本在 Plasma 链上，主链上的余额代表的是智能合约强制执行 Plasma 链本身的结果（译者注：相当于是 Plasma 链的帐户？））。灰色的项目是旧的区块，黑色的则是最近的被广播和提交到主链上的块。

不可想像的大量的交易可以提交到 Plasma 链上，只有非常少的数据落地到主链上。每一个参与方可以转移资产给任何人，包括转移给非当前存在的参与者。这些转移可以用主链的自身货币或代币支付或取现（需要一些时间上的延迟和证明）。

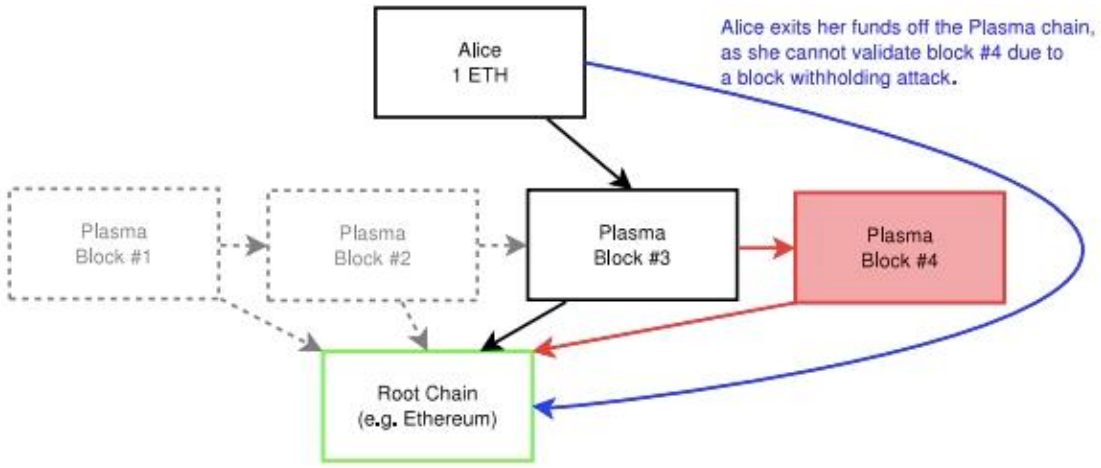
Plasma 允许大家（或者 Pos 网络的参与者）管理区块链，既不需要主链的一个完整的账本的备份记录，也不需要向第三方出示个人的信用信息。在最差情况下，资金被锁定，因为大量的退出，时间价值（time-value）丢失了。

我们在主链上构建了一系列的防欺诈的智能合约，来强制让状态在当前建立的通道内，由此试图进行欺诈，或者非共识（non-Byzantine）的行为可以大大的消减。

欺诈证明使用一种交互式的资金取款协议强制执行。与闪电网络类似，当取款时，取款行为需要申请一定的时间来到账。我们构建了一个交互式的游戏，退出方需要向参加者的帐本位图（账本内容是申请提现，结构是以 UTXO 模型）提交一个认证。在网络上的每个人都可以提交一个带押金的证明，来认证资金是否已经用掉。假如这是不正确的，网络上的任何一个人都可以举报欺诈行为，得到押金，回滚认证。在足够的时间之后，第二轮允许真正提现的押金回合开始了，押注在某个提交的时间戳前有效。这一轮允许批量的退出行为，保证一个有问题的 Plasma 链可以快速退出。对于批量的退出情况下，参加者也

能在消耗最多 2 位主链的区块链空间来实现退出（以太坊为例的最差情形下）。

当发生区块扣留攻击时，参与者可以快速和低成本的进行一个批量退出，能相比其它离线提案大幅的减少花费。额外的，这并不需要某些验证者节点的支持（侧链，polkadot 的 fishermen）



图三：当发生区块扣留攻击时的资金退出机制。红色的区块（Block #4）是一个被扣留，提交到主链上的区块，但 ALICE 不能访问到 Plasma 的区块 4。她将通过广播一个在主链上的资金证明来退出，他的取现只需要一点时间，因为需要公告以解决争议。

类似于闪电网络的在两方中结算的交互机制，支持强制的无限的双方之间的交易，Plasma 支持 n 方的交互。主要的区别在于不需要所有参与者在线来更新状态，参与者甚至不需要在主链上有一个记录项来参与进来-大家可以将资金放到 Plasma 链上，甚至不需要与主链直接交互，只需要以树状形式构建 Plasma 链时需要一点点交易确认数据。

2.2 区块链中的区块链的强制性

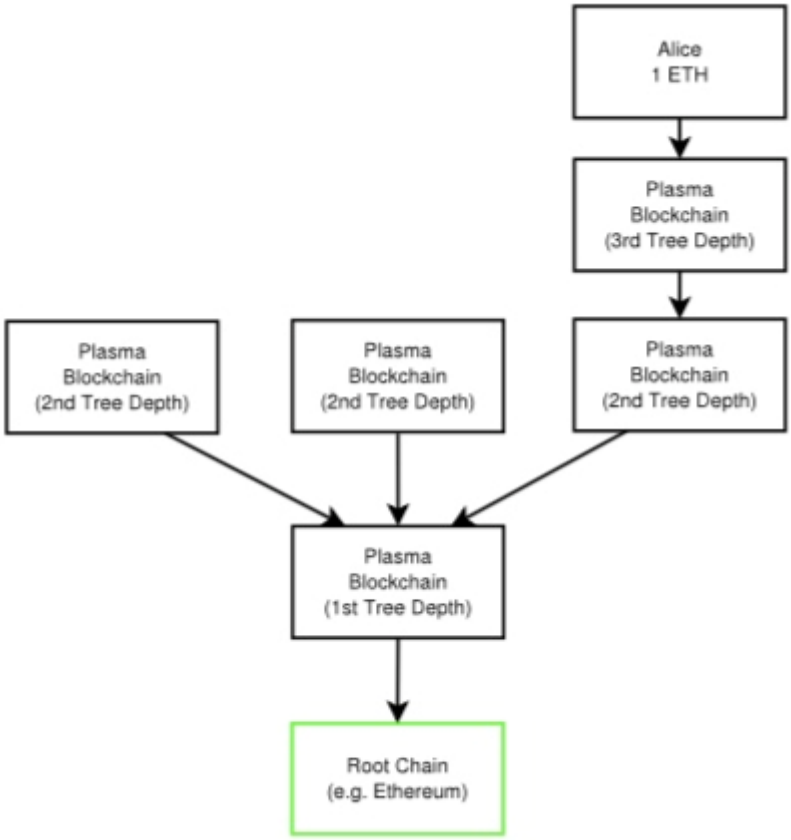


图 4：Plasma 以树状组织区块链。区块的提交依次向下流动。退出可以提交给任一父链。最终被提交到主链。

我们构建了一个类似法院的系统。如果闪电网络为支付建立了一个适配层，最终会在主链上强制执行。我们创建了一个更高层级的，下层法院来最大化可用性，最小化在非共识的状态下成本。如果一个链是 Byzantine 的，它可以选择去任何一个他的父链（包括主链）来继续他的操作或退出当前的提交状态。我们并未通过一个可以不断递增的现时状态（通过撤销状态），我们构建了一个欺诈证明机制来强制让余额或者状态迁移以分层的方式展示出来。

实际上，我们可创建状态迁移，仅仅只会周期性的提交到父链（最终将流向主链）。这将允许不可思议的计算能力和账户支持的扩张。因为我们能仅在 Byzantine 状态下提交原始数据到父节点（或者主链）。从有问题的 Byzantine 状态中恢复的成本将最小化，因为只需要去父 Plasma 链上申明某个状态。

子区块链运行于主链之上（主链可以是以太坊），从主链的角度来看，仅仅会看到在合约中有周期性的带代币押金的提交，用于强制运行 Pos 共识或者那个对应链的业务逻辑。

这一切的显著好处在于可以最大化区块的可用性，同时最小化验证某人的代币所需的押金。然而并不是所有的数据都传播到了所有的参与方（仅仅传播到了那些希望验证某个特定状态的），参与方有责任持续的周期性监控特定的链，那些他们感兴趣的，以在他们有欺诈行为时惩罚他们，同时也能在出现区块扣留攻击时，能自身快速的退出。

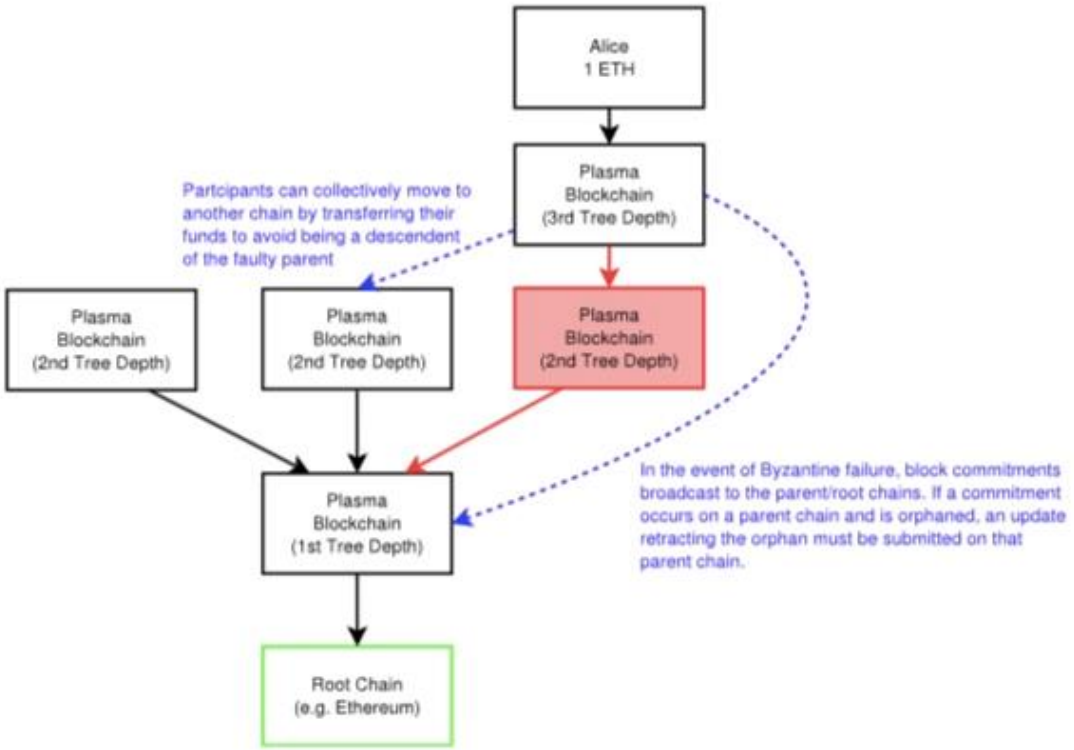


图 5：有问题的区块链（上图红色），通过提交到父 Plasma 链/主链（右侧的蓝色虚线）来绕过。在第三级的 Plasma 链的参与者，在一段时间后，进行了一个到其它链的批量迁移（左侧蓝色虚线）

这种构建在非 Byzantine 环境中，整合区块链状态树，同时更新所有的子 Plasma 链。横跨所有链的一整个状态更新集合可以经一个 32 位的签名来进行证明。

2.3 Plasma 的 Pos

通过一个单一的验证者，可以代表他人代持资金是一件非常有意思的事。我们提议一种方案，单方可以通过一系列的验证者来保证状态的确定性，通常在一个需要 ETH 或者代币为押金的框架下。

这个 Pos 系统的共识机制，再次，通过链上的区块链智能合约来保证他的确定性。

我们尝试复制 Nakamoto 共识，但是以 Pos 的押金形式。我们相信构成 Nakamoto 机制的其中一个更有用的激励机制是不可思议的激励来减少区块扣

留攻击（双花攻击，扣留 A 块，但打包另一个交易）。这也是最长链通过概率指定的原因。最长节点经过时间推移会概率性的被知道（最初的实现版本中是 6 个确认）。当人们发现一个区块时，大家也许会觉得他是最长的那条链，但也不是非常确定它是不是最长的。为保证它是最长的，他们附加自己的块并广播给网络中的参与者，来增大它的机率。我们相信如果它不是 Nakamoto 机制最关键的贡献的话，也是非常重要的，我们也在尝试复制这个激励。

Pos 整合面临着这个问题，如果人们直接选举新的主节点，进行主要节点进行区块扣留攻击（一般意义上的数据可用性），这个问题将非常可能被放大。

我们在 Plasma 的 Pos 中通过允许权益所有者在主链或父 Plasma 链中发布一个新区块的提交哈希来减轻这个问题。验证者仅会在他们完全验证过的节点上建新的区块，他们可以并行创建区块（为了鼓励最大化的信息共享）。我们创建了一个验主者的激励来让最近 100 个块与他们的当前的权益成正比（比如，如果一个节点的权益占 3 成，那么过去的 100 个块也需要占 3 成），通过对这种精确的表现奖励更多的交易费。超出的费用（基于那些表现不理想的权益者）将会进入一个池在将来支付费用。在每个块里存在一个提交包含最近的 100 个块（和一个 nonce）。正确的链将是总权重最高的链，一段时间后整个链将会确定下来（finalize）。

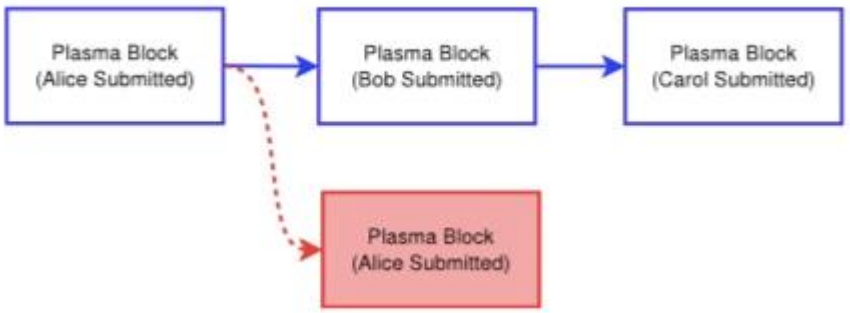


图 6：假设 Alice，Bob 和 Carol 是三个有相同权重的验证者。他们聚在一起构成一种轮循的结构来获得最大的收益。新的变化提交到了父或主链。链的末端是通过 n 个时期的正确分布后的最大权重分来偶然选定的（蓝色是当前的候选尾端节点，红色是个孤立节点）。次优链的末端的让所有的费用进行一个池，供正确性在某个阀值之上的验证者使用（比如阀值 90%）。在 n 个周期后，我们可以假设蓝色的链末端进入到确定状态。

这将鼓励大家参与进来，复制 Nakamoto 共识中的 51%攻击假设。当出现一个链被区块扣留攻击或者其它的 byzantine 行为，非 Byzantine 的参与者在父或主链进行一个批量的取款。如果最高的 Plasma 链的押金是用代币的形式，那么非常可能的，这个代币的价值将因为大量的退出而贬值。

2.4 区块链以 MapReduce 的方式

blockchain : git : Plasma : Hadoop

通过以 MapReduce 的格式来构建一个计算，以层级树组织的方式来设计计算状态迁移变得相对来说比较容易。

MapReduce 提供了一个框架来通过上千个节点进行高扩展计算。区块链面对着类似的问题，来达到这样的运算规模，同时需要额外的计算证明的生成。

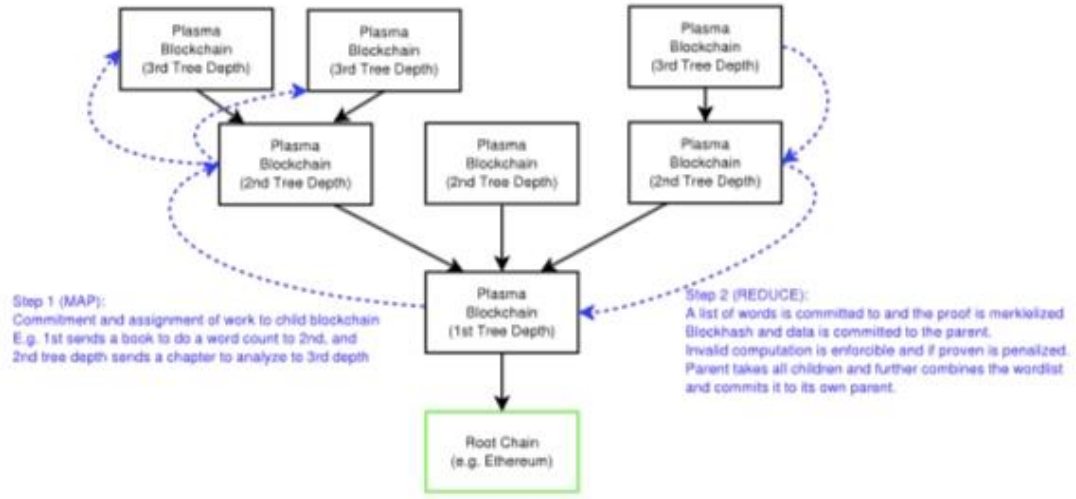


图 7：左侧蓝色虚线是 Plasma 从父节点传递到子节点的消息。子节点必须在 n 个节点内提交到父节点，否则链将暂停。向子链通过数据分发工作，子链提交工作证明。上图中，第三级的子节点完成这些计算，并返回一个字典表（比如，在他们需要计算的章节，统计出”hello“出现了三次等等）。结果字典表会做为提交的一部分被返回回来，字典表在子链中被组合并提交到父节点，最终完成一个全局的字典（比如，统计出整篇文章出现了 100 次”Hello“等等）。这创造了在大规模情况下强制计算执行的可能，只需要一个区块头提交到主链但却可涵盖大量的数据和工作。除需要发布某个区块是无效数据时，其它情况下仅需周期性的提交很小的数据量到主链。

我们提出了一个方法，Map 阶段把用于计算的提交数据做为输入，当返回结果时，在 reduce 里包含状态转换的 Merkle 证明。Merkle 状态迁移证明通过主链上构建的欺诈证明来保证会强制执行。当然构建一个 zk-SNARK 的状态转换证明也是可能的。对于某些计算的构建，状态迁移的 bitmap，在 reduce 步骤中也需要（由此每个 UTXO/账户在这些情况下会用超过一个 bit 位）。

上述的结构允许不可估量的高扩展计算，同时兼具时间和速度的权衡。这些权衡产生了一个网络，其中的节点假定计算的有效性，参与者有责任来校验他们。它不是一个这样的系统，大家可以无信任的输出计算能力，而是通过启用了一种能力，能把计算打包进一个绑定的押金证明上。这些绑定的证明鼓励参与者为诚实作证，否则将没收押金。再一次，跟随闪电网络的理念，如果一棵树落在森林中，没有人听他，我们会假设它并不重要，无论它是否产生了声响。类似的，如果没有人来关注/强制计算的执行，则假设它是正确的，或者它最终的结果是正确与否并不重要。计算可以被开放网络上的任何人关注，但利益相关者或者需要整个网络正确的运行的需要周期性的监督这个区块链来保证

正确性。扩展性的提升来源于移除了对不会对你产生经济影响的链的关注，人们应该只关注他们需要产生正确行为的链。同时，其它 Plasma 链的行为整体可以作为 reduce 步骤中的一部分网罗进来，由此影响到的某个人的其它计算会以最小状态表示。比如，在一个去中化的交易所，人们不关注谁会放入什么订单，它仅仅只会看到一个聚合的订单表，所以它需要把所有其它链看作一个第三方整体，来保证它当前的交易正确执行，最后订单就正确的人执行了（也包括它自身的）。另一个例子是，一个人可以在一个 Plasma 链上构建一个 BBS，它并不需要接收它不关心的主题的更新。

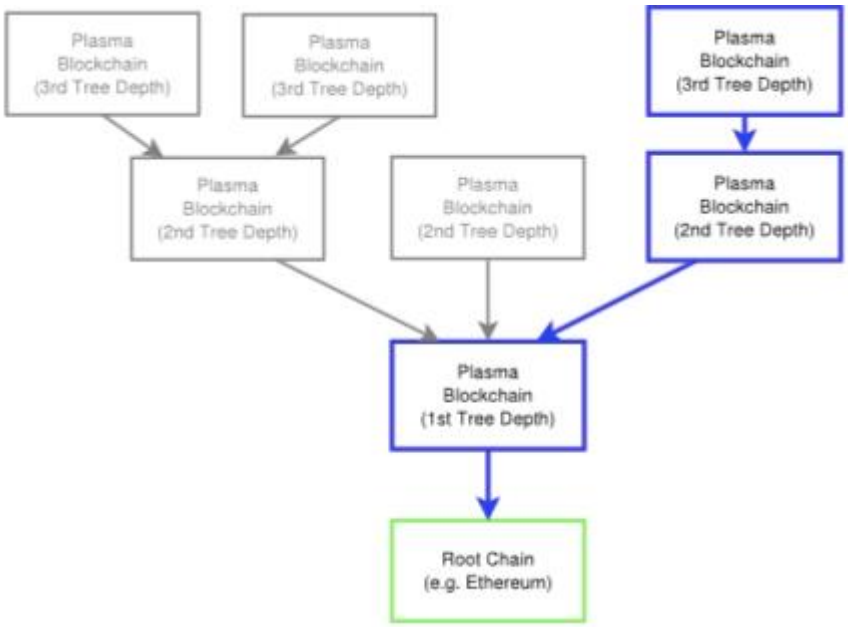


图 8：一个人仅仅需要关注那些他希望强制执行的数据。如果经济行为或者计算发生在其它的 Plasma 链上，它不需要强制执行的（灰色部分），它可以把所有其它链整体作为一个第三方。如，在一个 Plasma 的去中心化交易所，人们只需要关注影响到自己提交的链（蓝色粗线）。

2.5 关于持久化的去中化化的自治区块链的经济驱动

我们提议了一个结构，其中人们可以创建一个经济驱动，来激励子链永久的运行下去。对于不需要显著复杂性和依赖的状态转换，原生代币（如 eth 之于以太坊）可以用于状态转换的押金。然而，对于复杂的合约，如需要根据激励来确保在线或订单的公平性，则需要对持续运行进行重要的激励。

每一个 Plasma 链由一系列的合约表示。这些合约强制执行链上的共识规则，欺诈将导致严重的惩罚，如果能构造出欺诈的证明。

然而，为了激励避免出现 Byzantine 状态，尤其是保证正确性和可用性，理想情况下每个合约可以创建一个代币。代币代表的是运行这个合约的网络效应，同时创造了一个激励来最大化保证这个合约的安全。因为 Plasma 链运行于

Pos 的机制下，需要代币来保证网络的安全，权益相关者不被激励来赞同 Byzantine 行为或错误行为，因为这会降低所持代币的价值。代币在其中的角色是将成本本地化，因为它作恶，它的代币价值下降，影响的是他自己。

只是简单的合约和商业逻辑，比如代表它人持有资金的简单合约账户，以太坊押金可以用来在 Plasma 链中代表权益。

那些放上押金的权益者（无论是代币还是 eth）都被激励持续的运作网络，因为它们能收到交易费。这些交易费又被用来支付给网络中的权益相关者，从而又激励他们避免 Byzantine 行为，来创建一个拥有长期价值的代币。

由于权益相关者被激励来持续的运行网络来得到交易费，它们会持久的运行链，同时又受到主链中欺诈合约的约束。

3 设计栈和智能合约

从历史上看，大部分人相信匹块链的最佳适用场景是交易性的支付，比如利润结算系统。然而，我们意识到这样的结算系统很难扩展。而面向网络结算（net-settled）的设计，比如闪电网络，一个支付通道网络，改变了这个结构来允许参与者无限次的交易。渠道通过在区块链之上的网络结算（net-settled），交易容量可以显著的增加。支付可以路由到上述所说的渠道组成的网络进行处理。

这种结构还支持有效的即时支付。这对于无论是对时间高度敏感的支付，还是合约支付都非常有帮助。

Plasma 并不是设计来快速的达到确定态（finality），尽管交易可以在子链上得到快速的确认，但它仍需要在底层的主链上达到确定态（finality）。通道需要得到一个能快速返回的，虽然是子链的确定态（最终能在链上强制（enforcible））。

在智能合约中，有一个“自由选择问题（free option problem）”，智能合约的接收者（第二个或最后一个）需要最终对一个合约签名并广播以让其强制执行--但接收者也许会把它认为是一个可选项，如果没能吸引到它，它也许会拒绝执行上述操作。因为智能合约在处理不可信的第三方时最有效（因为交易对手风险越小，信息成本越小），这一点让上述情况尤为突出。

Plasma 并没能解决这个问题，因为区块链并没有一种交互协议能保证第一步和第二步签名的原子性。

闪电网络（包括基于 Plasma 之上的闪电网络），可以支持大量的更新，同时保证可接受的确定性。取代一次性的支付，一个支付可以被分成许多的小支付，支付仍需要最后参与方的选择。这可将自由选择的数额降到最低。由于智能合约的后续参与方，仅有拆分数额的自由选择权，自由选择的影响数量被最小化了。

基于上述的用例，闪电网络也许可以成为在 Plasma 之上，快速金融支付/合约的主要接口层，Plasma 可以只需要小量的主链账本更新。

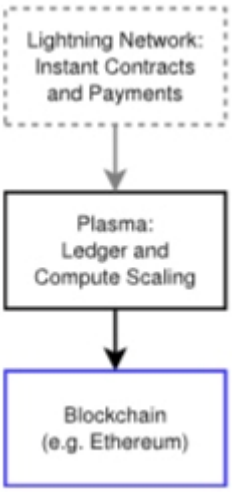


图 9：最底层是区块链，是合约和支付的判决层。合约本身在主链上。Plasma 链上包含了当前账本的状态，可以在主链上清算和赎回。如果存在欺诈将允许资金的赎回。Plasma 提供了一种链嵌套的结构，创建了一个场所，以最小的链上的交易，实现资金的可扩容的存取。闪电网络又基于其上，支持即时的支付。

3.1 分片（Sharding）最重要的问题是信息

在数据分片的情况下，极有可能单个分片的数据不足，从而无法生成欺诈证明。

我们尝试通过下述三个策略来解决这个问题：

1. 一个新的 Pos 的机制来鼓励区块数据的传播。底层机制并不需要完全依赖于激励。即使这样也将极大的减少欺诈行为。
2. 取款延迟是用来保证取款证明。个人不需要经常的关注区块链，出现错误行为的 plasma 链上的任何一个诚实的用户都可以在主链上终止这种行为。当区块扣留（block withholding）发生时，plasma 链可以立即通过一个证明锁定资金，阻止攻击者提交一个虚假的取款证明。当攻击者尝试在 Plasma 取款超出限额时，同时更多的资金将被锁定，被攻击的 plasma 链将失去他们的存款。
3. 创建子链，交易将经由此传递到父链。所以，网络中的参与者应该将交易提交到子链上。这提高了小额余额用户的经济效率，因为不用支付主链上的高额交易费，由此，许多的小额帐户中转移资产变得可能了。大家在使用时应该尽量使用足够深嵌套的子链，将会带来非常大的价值。请注意，对于持有非常小的余额用户，仍需要注意选择那些有较高信誉的链。安全模型是 plasma 链的关键创新。

4 相关工作

一些相关的项目提议使用一个精简步骤的梅克尔树（merkle tree）来作为计算证明（proof of computation），然而这个提议主要围绕数据可用性，支持降低欺诈证明的成本，通过经济驱动来进行区块链群的分片（sharding）持久化，他们使用一个协议来管理。

其它的一些相关工作提议一个子链系统，但在实现上有根本的不同。

Plasma 使用梅克尔证明（merkleized proof）来保证子链的强制执行。

4.1 TrueBit

Plasma 对于欺诈证明的想法极大的参考了 TrueBit[10]。欺诈证明的构建与 TrueBit 类似，几乎 TrueBit 上的所有成果可以直接应用于 Plasma，尤其是关于状态转移的梅克尔证明（merkleized proof）。

TrueBit 的设计允许创建精简的证明，来提交到以太坊区块链，其成果对 Plasma 来说非常需要。所以几乎所有 Truebit 白皮书涉及到的和团队完成的繁重的工作都可以直接应用到 plasma 的设计中。包括验证游戏（Verification Game），提供递增的奖励，以尽量少的计算规模的方式来生成梅克尔证明（merklized proof）。同时与 TrueBit 类似的假设也适用，即计算状态必须可计算且能在线上广播（大的数据块应该拆分到多个回合中），解决数据可用性的问题，失败状态能及时暴露。我们主要着力解决后两个问题。

Plasma 尝试基于 TrueBit 之上构建解决的主要问题是，多方需要在一个共享状态上完成计算。例如，一组参与者只关心一个数据的子集，计算也只应该计算与他们有关的部分（例如，BBS 或交易所）。我们也尝试通过链下的强制执行来解决需要回合式计算的场景。

4.2 区块链分片（sharding）

当前的区块链分片的工作，使用与以太坊分片提案类似的技术和目标。我们作为一个更高层级协议，可以兼容底层的分片机制（sharding）。如果主链是分片的，plasma 可以运行于其之上，获得扩展性和其它的好处。plasma 也可以成为不同分片技术的测试平台，因为在以太坊或其他的区块链中都不需要改变共识来支持 Plasma 链的基本运行。

4.3 联盟侧链（Federated Sidechains）

Plasma 不是一个联盟侧链[12]，因为 Plasma 并不需要联盟来保证诚实的行为，且也不需要在链内依赖诚实的参与者来强制状态。Plasma 同时也扩展了

其它区块链的账本状态来允许使用这种代币，然而如果欺诈证明可用的话，它会进行强制执行校验。因为 Plasma 并不依赖于参与者的强联盟，联盟链需要保证参与者的正确性，所以，它并不是一个联盟侧链。

Drivechains[13]使用类似联盟侧链的方案，仅仅在验证者上有所不同，使用了未知的，一个变化的参与者集合（矿工们），有更大的去中心化性。

4.4 联合挖矿区块链

例子包括 Namecoin，通过主链[14]来创建当前的区块。前提是需要对区块链的完整性进行校验，由此并不会带来扩展的好处。扩展区块是联合挖矿的另一个例子，它允许主链和联合挖矿链的资金的互相转移（要求主链上的矿工的共识来保证强制性）。联合链允许其它共识规则存在，通过选举用户来验证他们感兴趣的链，但矿工/验证者需要校验所有东西。Plasma 的目标是保证用户和矿工仅验证与他们有关的链。

4.5 Treechains

Treechains[15]提议了一个树结构的区块链，通过在子区块中使用 POW 证明进行校验。主链是所有子区块链的工作量证明的聚合。随着层级的降低安全性能较好的保证，随着层次的提升也许会或也许不会提升安全性，这取决于后续层级的验证级别和工作。因为 treechain 的拓扑图是一个树形结构，它的结构依赖于通过分支聚合的挖矿的安全性。这个安全模型在叶子节点有较低的安全性，因为它是 POW 保证的。Plasma 的安全性主要在根节点上，这点与之相反，安全性和证明从根流向叶节点。相类似的工作是以一个树形格式构建区块的证明。

4.6 zk-SNARKS 和 zk-STARKs

不需要交互的计算证明使得人们在可伸缩计算中获得显著好处[16]。zk-SNARKSs/STARKs 和其它形式的非交互式紧凑证明是 Plasma 的重要补充。他们可以提供一个梅克尔（merklized）计算的结果证明。另外，对于子链上持有小额帐户的情况来说，可以减少系统性攻击。在 SNARKs 中已经有了 MapReduce 功能的研究[17]，我们希望能够利用这一研究成果，Plasma 通过在一个区块链群中，提供有序的证明和执行的强制性扩展了它。

未来可支持的还有，允许更快的同步和校验链本身的计算证明。需要注意的是 zk-SNARKs 并没能解决数据可用性的问题，只是减少了需要的数据量和计算量。这可以作为任何基于时间的资产/挑战机制（asset/challenge time-based mechanisms）的替换或补充。zk-SNARKs 可以成为安全的一环，如果最后一层区块链的保护没有使用什么密码学特性，那么第二层保护可以是 zk-SNARKs，第一层保护是可信的计算机硬件。

从 plasma 链中取款会通过 zk-SNARKs 保证安全，带来的好处是可以选择性的不需要位图（bitmap），但在这种情况下仅允许小额的转移。

4.7 Cosmos/Tendermint

Cosmos[18]将区块链组织为一个个的 Cosmos 的 **Hub**，同时有名为 **Zones** 的子区块链，来实现对 pos 系统的校验。Plasma 与之在子链组织上有非常大的相似性，然而 Plasma 依赖于欺诈证明来保证子链上的状态的强制执行，同时也具有普适性适用于许多的链。Cosmos 的权益证明的构建假设 2/3 的验证者需要为诚实节点，其中包括 Cosmos 的 **Zones** 里的验证节点。

4.8 Polkadot

Polkadot[19]也构建了一个分层的区块链结构。Plasma 与 Polkadot 的设计有些相似之处。但我们使用了一系列的子链通过梅克尔证明来保证状态的执行，而不是使用类似 Polkadot 的 **fishermen** 的机制。Polkadot 的构建依赖于子区块链（parachains）的状态，状态的可用性由 **fishermen** 来保证。

4.9 Lumino

Lumino[20]是区块链上能压缩状态更新的 EVM 智能合约。这允许参与者仅仅更新最小的提交状态。Plasma 的输出管理的设计将这个事情推进了一步，只需要通过一个位来表示一个特定的输出。这允许在子 Plasma 链失败时，可以快速的，低成本的协调大量的取款操作。